REMARKS

Claims 1-27 are currently pending in the application. By this amendment, claims xxx are amended for the Examiner's consideration. The foregoing separate sheets marked as "Listing of Claims" shows all the claims in the application, with an indication of the current status of each .

The Examiner has rejected claims 1-9 and 11-27 under 35 U.S.C. §103(a) as being unpatentable over EP 0 908 810 A2 to Candelore et al. ("Candelore") in view of U.S. Patent No. 5,619,571 to Sandstrom et al. ("Sandstrom"). Claim 10 is rejected under 35 U.S.C. §103(a) as being unpatentable over Candelore in view of Sandstrom and further in view of U.S. Patent No. 5,745,643 to Mishina.

Candelore discloses an apparatus for efficiently and securely transferring blocks of program information between a secure circuit and an external storage device, where the program information is communicated in block chains for more robust encryption and to reduce authentication data overhead (col 1, lines 5-11). In this respect the disclosure is within the prior art as described in the background of the present invention. In Candelore, there is provision for encryption and authentication of block chains. In one embodiment, there is encryption with authentication being optional (col 1, lines 12-14); in another embodiment, there is authentication with encryption being optional (col 1, lines 15-17). But in this context both encryption and authentication refer to the basic program material being transmitted. Candelore discusses keys in connection with the encryption of program material, which is within the prior art (see col 4, lines 27-51 and col 11, lines 20-37). Candelore also provides for reordering of blocks to enhance security (col 1, lines 20-22), and for dependence of encryption keys upon a key that is unique to each decoder unit (col 31, lines 12-14 and lines 23-34).

The present invention is directed to the protection of movies and other programming transmitted to a mass storage device on a set-top-box (STB). The

context for the invention is existing digital audio and video transmission and reception standards and STB architectures, and an object of the invention is to provide an encryption technique that is compatible with this context (page 6, lines 3-5). It is also an object of the invention to provide an encryption technique that allows reduced data manipulation using a single key or a limited number of keys that can be securely handled in a simple manner, allowing playback on an authorized STB while preventing playback on different devices (page 6, lines 3-12). The technique of the invention provides for key usage in three particulars: defining a write order of data blocks to non-sequential storage locations in the mass storage device; allocating corresponding sectors in a file allocation table; and encrypting the file allocation table. Significantly, there is no need to authenticate a user, since the keys may be maintained internal to the decoder (page 7, lines 20-27).

The Examiner acknowledges that Candelore does not teach encrypting the table with a key, forming an encrypted table and storing the encrypted table in mass memory. The Examiner has indicated that Sandstrom provides a teaching of encryption of the table showing the storage locations of the data blocks. However, Sandstrom discloses a method for securely storing electronic records. The context of Sandstrom is the need in business to be able to establish that a particular electronic record was created or existed at a particular time (col 1, lines 23-24), and in particular to provide an alternative to the prior art technique of using the hash of the particular record at the particular time (col 2, lines 1-3). The alternative provided by Sandstrom is to combine an identification code and time data of the electronic record from a trusted source to generate a key which is then used to encrypt a private area, associated with the electronic record, containing a verification code (col 2, lines 15-25). There does not appear in Sandstrom any disclosure or suggestion related to the encryption of a storage location table. The Examiner's citations do not support the contrary assertion made in the office action.

In response the Examiner disagrees, arguing that the "information file directory" of Sandstrom discloses a storage location table. This is clearly incorrect, as may be demonstrated from the drawings and text of the Sandstrom reference. The citation used by the Examiner (col 5, lines 47-51) refers to item 54 in Fig. 2, which shows time data 62, an identification code 64, and a pointer 66. This is not a table, but rather identification entries (time, ID code and pointer) pertaining to a particular image file. It is clear that these entries are single valued (see col 4, lines 23-61), reflecting the time that the computer requested recordation of an image stream and a unique identification code associated with the image. Should the image be edited, a new image will be created (col 4, lines 55-56) so that an audit trail will be preserved for the image (col 4, lines 60-61). This is an implementation of the functionality described in Sandstrom, namely, the secure storage of electronic records. All the elements of Sandstrom's "file directory" are associated with a particular image. For one skilled in the art, there may be an analogy between a particular image in Sandstrom and a movie or other program material in Candelore. Applying that analogy, it is clear that the "file directory" entries are associated with an entity at the conceptual level of a movie or other piece of program material.

By contrast, the "storage location table" of the present invention pertains to entities at a completely different conceptual level, namely, the physical storage locations of an external storage device. It is likely that a particular image file under the Sandstrom scheme will be stored in physical storage media, and there may well be a plurality of physical data storage locations required for storage of the image file. It is possible that the pointer 66 in the Sandstrom file directory points to the first of these data storage locations. One skilled in the art would know that it is typical for there to be a table (e.g. a File Allocation Table) of pointers associated with these data storage locations, each pointer then pointing to the next data storage location where the storage of an image file is continued, and so on until the storage needs of the image file are exhausted. Without this (or some equivalent) mechanism for storing a

sequence of pointers to the data storage locations, it would be impossible to recover the image file. Only in the narrow case where the image file is small enough to fit within a single data storage location could it be argued that the single pointer 66 entry could be construed as a "storage location table." Further, it is to be observed that the "private area" which is encrypted is specific to the particular image file. Each image file has its own "private area" having at most a single pointer entry 66, and therefore there is no possibility of a suggestion from Sandstrom of encrypting a single file containing a plurality of pointers, much less a sequence of file location pointers necessary to reconstitute a file of program material stored in a plurality of file locations.

It would be meaningless to scramble a one entry table. This is not to say that, under the present invention, security could not be provided to a media file occupying only a single data storage location. This is so because, under the present invention and in the relevant practice known to those skilled in the art the table itself is a separate entity from any stored program material and has a plurality of entries, each of which would be remapped when the table itself is scrambled using a key. It should be emphasized that this is an entity different from the "file directory" described in Sandstrom. It is sufficient for removal of Sandstrom as a reference for this aspect of the invention to note that there is no suggestion in Sandstrom that its "file directory" is a table of file location pointer entries that may be scrambled and then encrypted. The claims have been amended to make this clear.

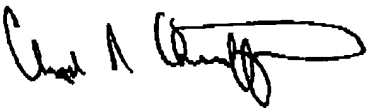
Consequently, the Examiner's acknowledgment that Candelore fails to teach encryption of the storage location table with a key is sufficient to remove Candelore as reference, with or without the combination of Sandstrom. This applies to independent claims 1, 14 and 25, and all the claims dependent therefrom, all of which contain the element of key encryption of a storage location table. This includes claim 10, making it unnecessary to consider the Mishina reference.

In view of the foregoing, it is requested that the application be reconsidered, that claims 1-27 be allowed, and that the application be passed to issue.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at 703-787-9400 (fax: 703-787-7557; email: clyde@wcc-ip.com) to discuss any other changes deemed necessary in a telephonic or personal interview.

If an extension of time is required for this response to be considered as being timely filed, a conditional petition is hereby made for such extension of time. Please charge any deficiencies in fees and credit any overpayment of fees to Deposit Account 09-0457 (IBM-Endicott).

Respectfully submitted,



Clyde R Christofferson
Reg. No. 34,138

Whitham, Curtis & Christofferson, P.C.
11491 Sunset Hills Road, Suite 340
Reston, VA 20190
703-787-9400
703-787-7557 (fax)

Customer No. 30743